

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

JEFFREY LAYDON, on behalf of himself and all  
others similarly situated,

Plaintiff,

-against-

MIZUHO BANK, LTD., THE BANK OF TOKYO-  
MITSUBISHI UFJ, LTD., THE SUMITOMO  
TRUST AND BANKING CO., LTD., THE  
NORINCHUKIN BANK, MITSUBISHI UFJ  
TRUST AND BANKING CORPORATION,  
SUMITOMO MITSUI BANKING  
CORPORATION, RESONA BANK, LTD., J.P.  
MORGAN CHASE & CO., J.P. MORGAN CHASE  
BANK, NATIONAL ASSOCIATION, J.P.  
MORGAN SECURITIES PLC, MIZUHO  
CORPORATE BANK, LTD., DEUTSCHE BANK  
AG, MIZUHO TRUST AND BANKING CO.,  
LTD., THE SHOKO CHUKIN BANK, LTD.,  
SHINKIN CENTRAL BANK, UBS AG, UBS  
SECURITIES JAPAN CO. LTD., THE BANK OF  
YOKOHAMA, LTD., SOCIÉTÉ GÉNÉRALE SA,  
THE ROYAL BANK OF SCOTLAND GROUP  
PLC, ROYAL BANK OF SCOTLAND PLC, RBS  
SECURITIES JAPAN LIMITED, BARCLAYS  
BANK PLC, CITIBANK, NA, CITIGROUP, INC.,  
CITIBANK, JAPAN LTD., CITIGROUP GLOBAL  
MARKETS JAPAN, INC., COÖPERATIEVE  
CENTRALE RAIFFEISEN-BOERENLEENBANK  
B.A., HSBC HOLDINGS PLC, HSBC BANK PLC,  
ICAP PLC, R.P. MARTIN HOLDINGS LIMITED  
AND JOHN DOE NOS. 1-50,

Defendants.

Docket No. 12-cv-3419 (GBD) (HBP)

ECF Case

**DECLARATION OF HIROTAKA URANAKA**

I, **Hiroataka Uranaka**, pursuant to 28 U.S.C. § 1746 and upon penalty of perjury under the laws of the United States of America, declares that the following is true and correct to the best of my knowledge:

**Background and Qualifications**

1. I am an attorney, duly admitted to practice law in Japan. I was admitted to the Japanese bar and began practicing law in 1997 (Attorney Registration #25144).

2. I am currently a partner of the law firm of Iwata Godo in Tokyo, Japan. At Iwata Godo, I practice and specialize in areas including commercial litigation representing Japanese banks and various bankruptcy matters. I also have experience in advising Japanese banks and other types of financial institutions often on matters relating to the protection of personal information/customer information held by them in regulatory and transactional contexts. A *curriculum vitae* which generally sets out my professional qualifications and experience is annexed hereto as Exhibit 1.

3. I am admitted to practice law in New York State as well, having been registered since 2003 (Attorney Registration #4176483).

4. I am familiar with the facts stated in this declaration based on my experience practicing law in Japan.

5. The purpose of this declaration is to advise the Court of the existence of the Act on the Protection of Personal Information of Japan, explain its purpose and content, with a particular focus on the provisions addressing disclosure to third parties, and describe the potential penalties that can be imposed for non-compliance. The declaration also aims to describe how a business operator can make disclosures in foreign (i.e., non-Japanese) juridical proceedings in circumstances, such as the one presented here, where obtaining the consent of the individuals whose personal information will be subject to disclosure is impossible or impractical.

**Japan's Data Privacy Law**

6. The Act on the Protection of Personal Information of Japan (Act No. 57 of May 30, 2003, as amended; "APPI") is the principal data protection legislation in Japan for the protection of personal information. The English translation of APPI which is published by the

Ministry of Justice of Japan on the website of “Japanese Law Translation Database System” at <http://www.japaneselawtranslation.go.jp> is annexed hereto as Exhibit 2.

7. Based on Articles 8 and 36(1) of APPI, each administrative ministry regulating specific industrial sectors issues data protection guidelines for those sectors to ensure the implementation of the APPI. With regard to the banking sector, the Japanese Financial Services Agency (“JFSA”) issued guidelines in November 2009 (the most recent update was made in July 2015) to ensure the appropriate and effective implementation of measures to be taken by financial institutions such as banks (“APPI Guidelines”) in handling and protecting personal information.

**Scope and Restriction of Provision of Personal Information under APPI**

8. The purpose of the APPI is to protect the rights and interests of individuals while taking consideration of the usefulness of personal information, in view of a remarkable increase in the utilization of personal information due to the development of advanced information and communications technology in society, by prescribing the duties to be observed by entities handling personal information and the proper handling of personal information.

9. Though the terms “personal information” and “privacy” are not explicitly stipulated in the Constitution of Japan, the Supreme Court of Japan has considered the right to privacy as one of the critically important personal rights which are based on “the right to life, liberty, and the pursuit of happiness” under Article 13 of the Constitution of Japan. In 2003, for example, in a civil tort case where university students claimed damages from a private university which submitted a list of the students attending a speech of the Chinese President held in the university to the Japanese police for the purpose of guarding Chinese officials in attendance, the Supreme Court of Japan held that student numbers, names, addresses and telephone numbers on the list shall be protected as personal information relating to the plaintiff’s privacy and therefore the provision of the list to the police without prior consent constituted a tort (Saikō Saibansho [Sup.Ct.] Sep.12, 2003, Hei 15 (kyo) no.8, 57 Saikō Saibansho Minji Hanreishū 973 (Japan)).

10. The APPI defines the term “personal information” broadly as “information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy

reference to other information and will thereby enable the identification of the specific individual).”

11. APPI Guidelines further define sensitive information as information on political views, religion (meaning thoughts and creed), participation in union activities, race, family origin and registered domicile, health care, sex life and past criminal records. (Article 6-1 of APPI Guidelines)

12. Under APPI, a business operator in Japan handling personal information shall not, except in the cases mentioned in paragraphs 16 and 17 below, provide personal data (which means the personal information constituting a personal information database, i.e., personal information that is retrievable or searchable through a computer database etc. used by the business operator) to a third party without obtaining the prior consent of the person (the main clause of Article 23(1) of APPI). A business operator includes any business entity in Japan using a personal information database, etc. for its business in which personal information identifying more than 5,000 specific individuals is included on every single day in the last six months. Because the personal information of specific individuals is not limited by the type of individual (e.g., customers) and includes any type of individual (e.g., employees, shareholders), a Japanese bank or a foreign bank with operations in Japan is plainly a business operator within the meaning of the APPI.

13. APPI Guidelines confirm the above general prohibition on provision of personal data to a third party under APPI and strengthen it by stipulating that the prior consent of the person shall be, in principle, in writing and also that the person giving consent should be well-informed in such written consent of (i) the third party to whom the personal information will be provided, (ii) the purpose of the third party for the personal information, and (iii) the content of the personal information to be provided (Article 13-1 of APPI Guidelines).

14. APPI Guidelines also clarify that the third party under Article 23 of APPI means any third party regardless of natural persons or judicial entity, other than the business operator which is providing the personal data and the person whose personal information is to be provided (Article 13-2 of APPI Guidelines). Therefore, even if a certain measure is taken so that personal data is provided to a limited range of third party recipients (such as attorneys at law who have statutory duty of confidentiality), such an arrangement still constitutes the violation of APPI.

15. Further, APPI Guidelines require financial institutions to take safety control measures to prevent leakage of personal information held by them, such as organizational safety control measures, personnel safety control measures, and also to supervise its directors, auditors, officers, and employees to ensure the safety of personal data/information.

**Exceptions to General Prohibition of Provision of Personal Information under APPI**

16. The general prohibition on provision of personal data to a third party without obtaining the prior consent of the individual whose personal information is subject to disclosure under the main clause of Article 23(1) of APPI is lifted only in the following exceptional cases (Article 23(1));

- (i) if the provision of personal data is based on laws and regulations;
- (ii) if the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person;
- (iii) if the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person;
- (iv) if the provision of personal data is necessary for cooperating with a national organ, a local government, or an individual or a business operator entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of the affairs.

17. In addition, APPI also allows personal data to be provided to a third party if the so-called opt-out measures are arranged before the provision. Article 23(2) provides that a business operator handling personal information may provide personal data to a third party if the business operator, prior to the disclosure of the personal data, notifies the person of (i) the fact of the provision to a third party is the purpose of utilization of the information, (ii) the items to be provided to a third party, (iii) the method of provision to a third party and (iv) that the provision will be discontinued at the request of the person. However, if the purposes of utilization of information, which shall be publicly announced or notified to the person when the information is

collected under Article 18 of APPI, do not include the provision of the information to a third party as well as its purpose, the opt-out measures may not be taken (use of information beyond the scope of the purpose of utilization notified/announced when the information is collected violates Article 16 of APPI).

18. The above opt-out arrangement still requires (tacit) consent of the person whose personal information is to be provided to a third party. Therefore, the business operator may not provide personal data to a third party if the person whose personal information is to be disclosed requests the business operator not to provide such data.

19. As a matter of practice in Japan, business entities often rely on the exception of “based on laws and regulations” under Article 23(1)(i) of APPI above in order to provide personal data to a third party without violating APPI. However, this exception is considered inapplicable to the case where a business operator handling personal information is required by foreign laws or regulations to provide personal information. JFSA publicly released on December 28, 2004 on its website at <http://www.fsa.go.jp/news/news/16/f-20041228-4.html> its interpretation of the meaning of “laws and regulations” under Article 23(1)(i), in response to question no.8 raised during the public comment process in preparation for the draft of APPI Guidelines. The English translation of the JFSA’s interpretation is as follows.

*It is interpreted that the words “based on laws and regulations” stipulated under Articles 16(3)(i), 18(4)(iii), 23(1)(i), and 25(1)(iii), etc. of the Act on the Protection of Personal Information do not include foreign laws and regulations. Since the Guidelines are issued based on the Act, the Guidelines are applied in accordance with such interpretation.*

20. The JFSA’s interpretation mentioned in item 19 above that the “laws and regulations” under Article 23(1)(i) of APPI do not include foreign laws and regulations is reflected in Article 13-1 of APPI Guidelines that cross-reference to Article 5(3)(i) of the Guidelines which provides examples of “laws and regulations” based on which the provision of personal information to a third party without consent is exceptionally allowed. The examples in Article 5(3)(i) only refer to Japanese laws/statutes such as the Act on General Rules for National Taxes (Act No. 66 of April 2, 1962), and Code of



Criminal Procedure (Act No. 131 of July 10, 1948), etc., and does not include any foreign law or regulation.

21. Therefore, for at least banks and financial institutions that are subject to APPI Guidelines, they may not rely on the “laws and regulations” exception under Article 23(1)(i) when they are requested to provide personal data based on foreign laws or regulations.

**Permissibility of Redacting Personal Information from Documents Proposed Produced to Third Parties**

22. In some circumstances, it is impossible or impractical for business operators handling personal information to obtain consent or to rely on exceptions stated in paragraphs 16 and 17 for provision of personal data to a third party.

23. In such case, business operators can elect to anonymize (including, through redaction) personal information from documents to be disclosed to third parties in order to follow the request for disclosure without violating the APPI.

**Signatory Status of Hague Evidence Convention and U.S.–Japan Bilateral Treaty**

24. Since Japan is not a signatory to Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, Japan as a sovereignty, is not obliged by means under the Convention such as a letter of request by a judicial authority of a foreign state, to obtain evidence in Japan for the purpose of use in judicial proceedings in the requesting foreign state.

25. Therefore, a request by a foreign court to a competent authority of Japan, in accordance with said Convention, to provide documents which include personal information protected under APPI does neither impose any obligation on Japan nor constitute an exception to the general prohibition of provision of personal data to a third party under APPI.

26. The U.S.-Japan Consular Convention of 1963, a bilateral treaty between the U.S. and Japan, gives authority to U.S. consular officers to do some evidence-taking activities in Japan. However, under Article 17(1)(e)(ii) of the Convention, U.S. consular officers are authorized to take depositions in Japan on behalf of the courts or other judicial tribunals or authorities of the U.S. only if the depositions are “voluntarily given” and in accordance with the laws of the U.S. and in a manner not inconsistent with the laws of Japan. With regard to the U.S.

consular officers' documents obtaining exercise in Japan, Article 17(f) of the Convention authorizes U.S. consular officers to obtain copies or extracts of documents which are publicly stored only and it does not authorize them to obtain other documents in Japan.

**Measures for Compliance and Penalty for Non-Compliance with APPI**

27. The competent minister (for banks this is the Commissioner of JFSA) may recommend, if a business operator handling personal information has violated any of the provisions of Article 16 to Article 18, Article 20 to Article 27, or Article 30(2) of APPI, that the business operator cease the violation and take other necessary measures to correct the violation when a competent Minister finds it necessary for protecting the rights and interests of individuals (Article 34(1) of APPI). The competent minister may go further to order the business operator to take the recommended measures if the business operator does not take the recommended measures without justifiable ground and if the competent minister finds that the serious infringement on the rights and interests of individuals is imminent (Article 34(2) of APPI).

28. In addition to the above recommendation and order, the competent ministry may, if a business operator handling personal information has violated any of the provisions of Article 16, Article 17, Articles 20 to 22, or Article 23(1) and the competent minister finds it necessary to take measures urgently due to the serious infringement of the rights and interests of individuals, order the business operator to cease the violation and take other necessary measures to rectify the violation (Article 34(3) of APPI).

29. If a business operator handling personal information does not take the necessary measures ordered by the competent ministry, the person shall be sentenced to imprisonment with work of not more than six months or to a fine of not more than 300,000 yen (Article 56 of APPI). If any representative of a jurisdictional person or any agent, employee or other workers of a jurisdictional person is punished, such judicial person shall also be sentenced to the same amount of said fine (Article 58).

30. APPI Guidelines provide that in determining whether to issue the recommendation under Article 34(1) of APPI, or orders under Article 34(2) or (3) of APPI, the JFSA will take into consideration whether a financial institution has taken necessary measures in accordance with APPI Guidelines (Article 24(1) of APPI Guidelines).



**Proposed Amendment to APPI**

31. On March 10, 2015, the bill to amend APPI was submitted to the 189th ordinary legislative session of the National Diet of Japan which consists of the House of Representative and the House of Councillors. Though the bill was passed at the House of Representative and submitted to the House of Councillors on May 21, 2015, it is reported that the deliberation of the bill at the House of Councillors has been suspended principally due to the incident of a leak of national pension related personal information. If approved, most of the proposed amendments to APPI will take effect on a date designated by the cabinet within two years after the date of promulgation.

32. The bill to amend APPI provides for amendments facilitating the use of personal data while strengthening the protection of privacy. Some of the significant proposed amendments to APPI include:

(i) Expanded definition of “personal information”

The bill expands the definition of “personal information” by adding two types of personal information: (1) letters, numbers, and any other code converting physical characteristics of specific individuals and (2) letters, numbers, and any other code provided in relation to services or goods provided to individuals or those in documents to be issued to individuals which could identify specific individuals.

(ii) Special consideration for “sensitive information”

The bill recognizes sensitive information of a person such as race, creed, social status, history of diseases, past criminal record, and the fact that the person is a victim of a crime, and prohibits business operators handling personal information (1) from obtaining “sensitive information” without prior consent of the person, or (2) from providing such sensitive information by way of the opt-out arrangement under Article 23(2) of APPI.

(iii) Provision of anonymized information

The bill allows the provision to a third party of personal data, without the requirement of first obtaining consent, if it is processed so that the processed

information can no longer identify specific individuals and cannot not be restored to the personal information.

(iv) Extraterritorial transfer of personal data

The bill amending APPI provides for additional requirements for extraterritorial transfer of personal data. Under the proposed amendment, one or more of the following conditions must be met in order to transfer personal data to a third party outside Japan: (1) the personal data is transferred to a jurisdiction that has been certified to have data protection standards equivalent to those of Japan for the protection of personal rights, (2) the personal data is transferred to a third party outside Japan which has been certified to have such safety control measures as designated separately and equivalent to those taken by business operators handling personal information pursuant to APPI, or (3) the person whose personal information is transferred to a third party gives prior consent to the extraterritorial transfer of the information.

Tokyo, Japan  
August 5, 2015

  
Hirotaka Uranaka